EXHIBIT 4

EXHIBITS A THROUGH K
INTENTIONALLY OMITTED

EXHIBIT L

Exhibit L

NARUS®

UNIFIED IP MANAGEMENT AND SECU

SOLUTIONS
IP Security
» NarusSecure
IP Monitoring
» NarusLI
» NarusDA
» NarusForensics
IP Analysis
» NarusAnalyze
» NarusView
IP Mediation
» NarusMediate
NARUS IP PLATFORM
PRESS ROOM
ABOUT NARUS
CONTACT
RESEARCH FELLOWS

Home » Solutions

IP Analysis

Carrier and governr networks rely on Na to provide them the to analyze their netu and customer traffic

One distinctive capability that Narus is known for is its ability to capture and collect data at true carrier speeds. Every second, every minute and everyday, Narus collects data from the largest networks around the world.

To complement this capability, Narus provides analytics and reporting products that have been deployed by its customers worldwide. They involve powerful parsing algorithms, data aggregation and filtering for delivery to various upstream and downstream operating and support systems. They also involve correlation and association of events collected from numerous sources, received in multiple formats, over many protocols, and through different periods of time. All of this is displayed in interactive and intuitive graphical user interfaces.

NarusAnalyze

NarusAnalyze provides the real-time ability to capture, analyze and correlate Layer 3 to Layer 7 network and customer data and generate statistics, reports and information that enable key business decisions.

NarusAnalyze includes **VoIP Analysis**, an enhanced offering that is helping global carriers understand and address the impact of VoIP traffic on their business, and empowers them to generate revenue out of VoIP bypass traffic.

NarusView

NarusView delivers a 360-degree view of network systems, services and customer activity through a powerful interactive tool that provides business metrics, visual multi-dimensional analysis, reporting, presentation, monitoring and alerting capabilities.

Customers

- **U.S. Cellular** uses **NarusView's** powerful analysis and drill down capabilities to maintain a competitive network and create a marketing advantage.
- **Telecom Egypt** uses **NarusAnalyze** to detect and manage traffic on their network in real time.

Learn more » NarusAnalyze | NarusView

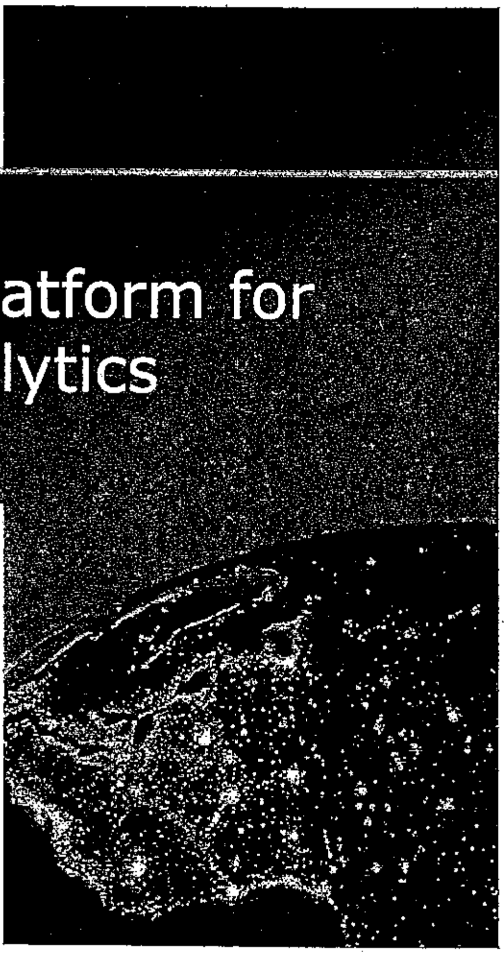
HOME · SOLUTIONS · NARUS IP PLATFORM · PRESS ROOM · ABOUT NARUS · CONTACT · RESEARCH FELLOWS

EXHIBIT M

Exhibit M

IP Platform behind the largest,
most profitable networks

Configurable IP Platform for Network Analytics



NARUS presentation to SCAMPI

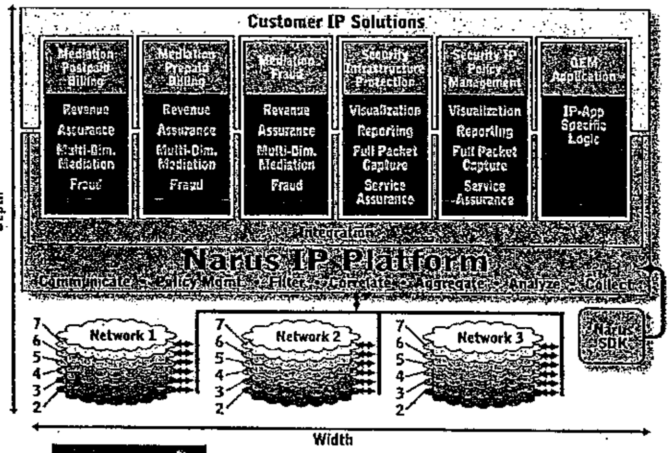
Georg Pöll/Andrew Cockburn

May, 2004

NARUS®

Carrier Class IP Platform for the largest, most profitable networks in the world

NARUS



"Total Network View" decision making through the real time collection and analysis of one packet to billions of packets across multiple networks

Customers and Partners extend NARUS' IP Platform with IP Application including Mediation, Security, and others

Bull

DATACRAFT

KT "The Value Networking Company"

T · · Mobile · Get more from life

AT&T

kpn

KDDI

NEC

Sofrecom

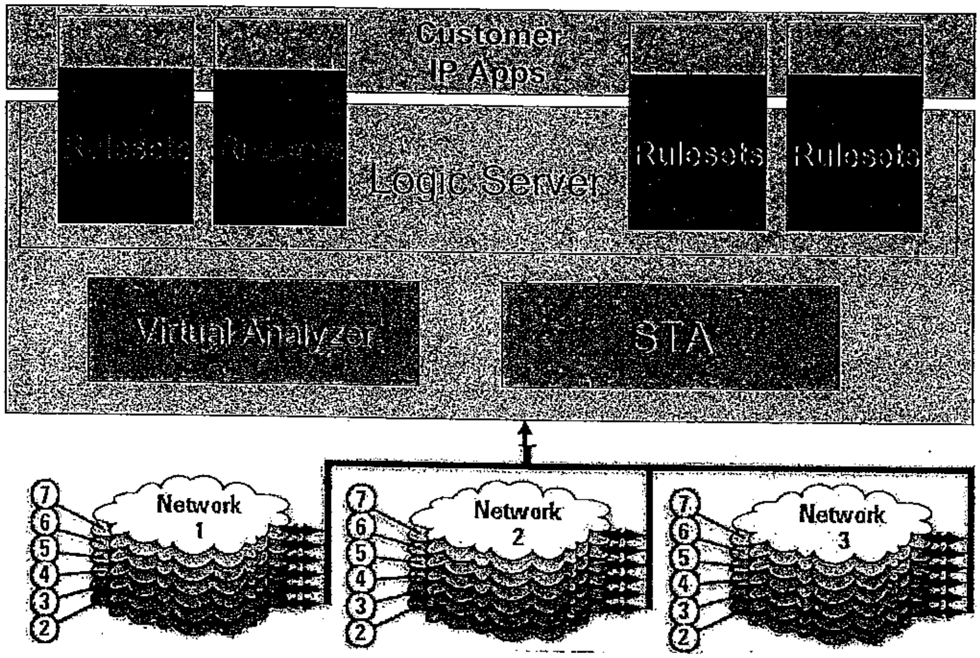
US Cellular

المصرية للاتصالات Telecom Egypt

· · T · · Systems ·

NARUS

Narus Product Configuration - Technical View

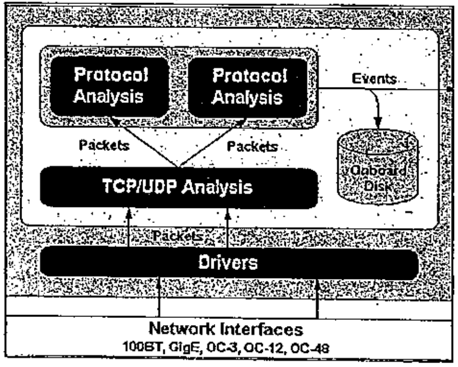


Proprietary and Confidential

Narus Traffic Aggregation and First Level Analysis

STA

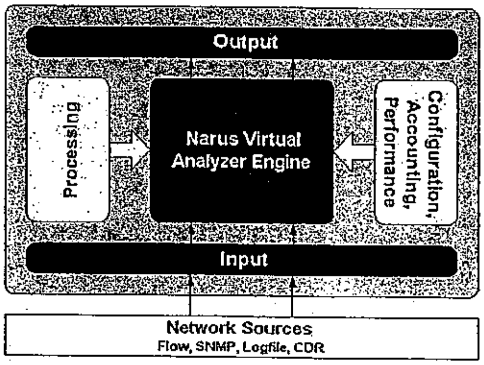
Semantic Traffic Analyzer



- Network transparent collection and semantic analysis of traffic
- Captures detailed, protocol-specific data in addition to collecting standard data
- Interfaces directly to the network using Narus Semantic Traffic Analysis™ technology

VA

Virtual Analyzer

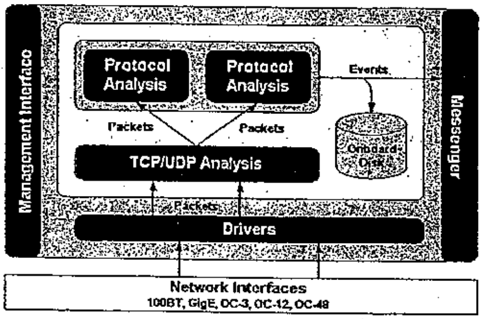

Output
Processing
Narus Virtual Analyzer Engine
Configuration, Accounting, Performance
Input
Network Sources
Flow, SNMP, Logfile, CDR

- Extracts information from network devices and service elements using standard protocols:
  - SNMP
  - Voice Mediated CDRs
  - CGF
  - LDAP
- Highly configurable with the Narus VA Toolkit

Narus Semantic Traffic Analysis

Captures detailed, protocol-specific data in addition to collecting standard data directly from the network using Narus® Semantic Traffic Analysis™ technology.

- Extracts information directly off the wire
- Not a sniffer: session modeling and reconstruction
- Detailed visibility into user traffic
- Network transparent, non-intrusive



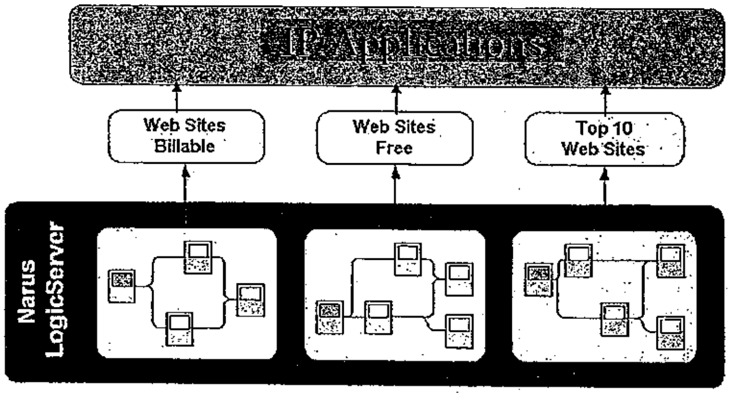
Vendor and protocol independent: IP standards based

Highly tuned appliance: 300-500Kbps

Network efficient: 95-99% data reduction

Network transparent collection and semantic analysis of traffic

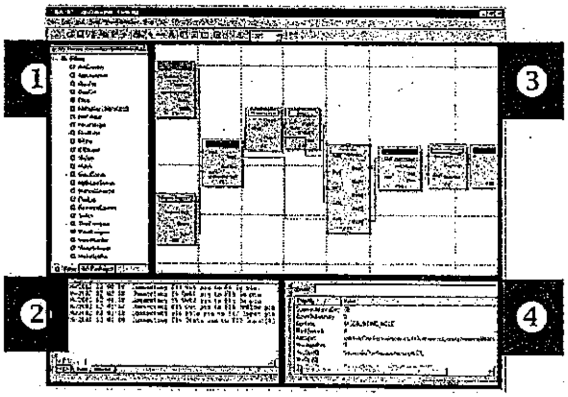
Narus LogicServer
Rules Based Correlation and Analysis



Executes Narus RuleSets in real time

- RuleSets represent the desired business rules
- Event-driven, in-memory, data-flow engine
- High-performance, low-latency, on-the-fly analysis

Narus Developer's Studio



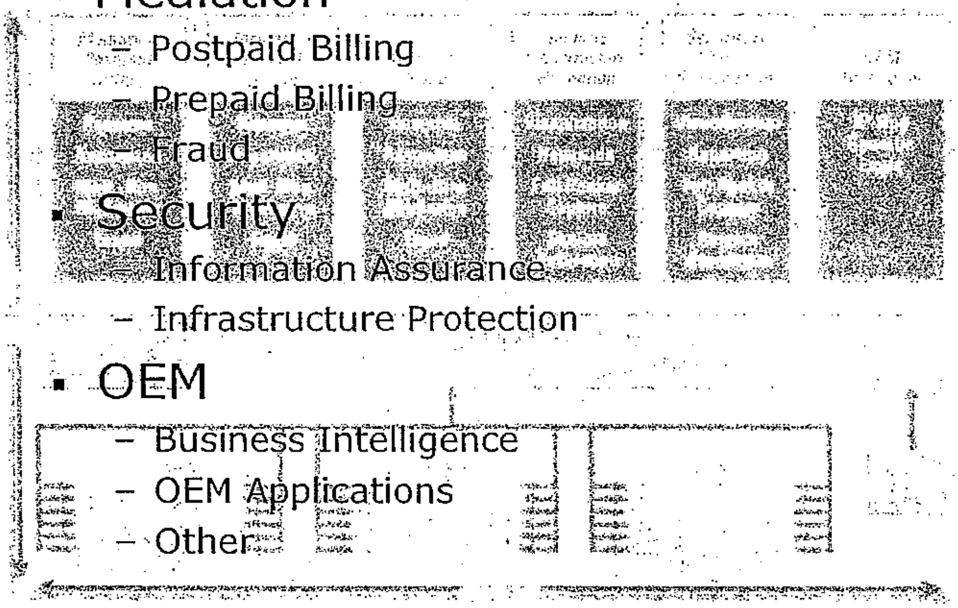
- ❶ Filters and Filter Packages
- ❷ Output window
- ❸ Filters grouped to form RuleSets
- ❹ Filter properties

- Flexible Aggregation and Filtering
  - Arbitrary keys and time intervals
  - Concentrator: multiple in, single out
  - Splitter: single in, multiple out
  - Boolean XOR, NAND, IOR
  - Relops =, !=, <, >, =>, =<, !<, !>
- Merging multiple instances as defined by arbitrary key values
  - Within single or multiple data streams
  - Same or different classes of data
- Categorization
  - Logical "Case" structure
  - Based on object attribute value, or function output
- Correlation
  - Create linkages between asynchronous data streams and other data sources
  - RADIUS, DHCP, LDAP, Database, DNS, Flat Files...

Create, modify, extend analysis to meet expanding needs and address new services

NARUS Enabled IP Applications

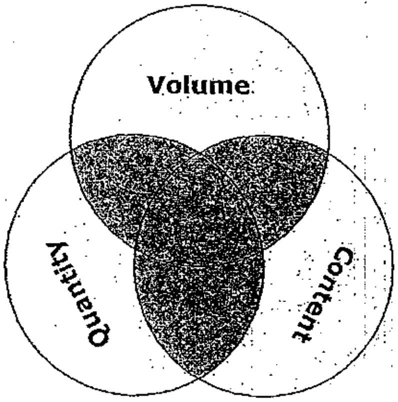
- Mediation
  - Postpaid Billing
  - Prepaid Billing
  - Fraud
- Security
  - Information Assurance
  - Infrastructure Protection
- OEM
  - Business Intelligence
  - OEM Applications
  - Other



Customer IP Solution reference designs

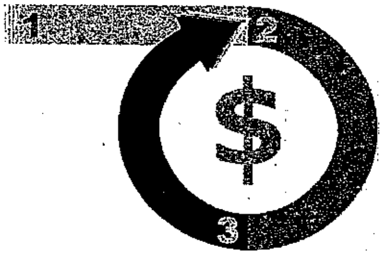
Postpaid Billing

- Narus System configuration for billing for value-based data services
  - Facilitates rapid revenue capture
  - Speeds service deployment
  - Ensures proper ongoing billing plan management
  - Leverages existing infrastructure
    - Uses production 3rd party billing applications
    - Interfaces with any number of network elements
- Flexible information processing
  - Multiple billing plan variants
    - Total volume or volume per consumed application
    - Quantity of events
    - Detailed content usage
  - Enables rapid changes as user trends change



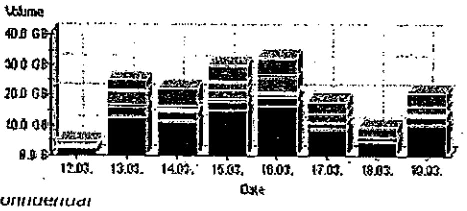
Prepaid Billing

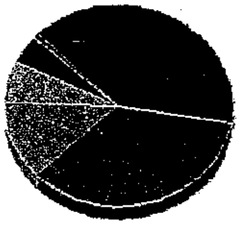
- Narus System configuration to provide revenue assured prepaid data service
- Focuses on the customer experience
  - "Soft Landing" – subscriber redirection
  - Flexible enforcement mechanism
  - Ensures access to selected "free" sites, even with a zero balance
  - No impact on un-enforced quality of service
  - Immediately brings customer back to where they were enforced after exhausted balance is updated
- Enables single balance source for converged offerings
  - Voice and data
  - Prepaid and postpaid



Fraud

- Narus System configuration to detect and manage fraud
  - Designed for mobile networks
  - Captures usage data for delivery to a central database
    - Integrated with Business Support Systems
  - Analyzes IP traffic by content and categorizes the applications being used
- Key features
  - Information on customers' service usage
  - Assistance with network optimization
  - Alarm generation as thresholds are reached
  - API to common reporting tools





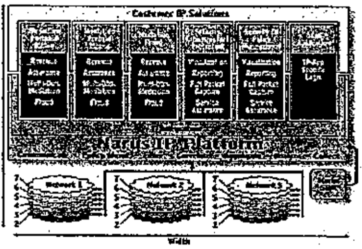
IP Policy Management

- Narus system Configured for Real-time network analysis
  - Normalizes across large networks, carrier grade
- Determines usage patterns
  - Collects and categorizes network usage from Network to Application layers
  - Programmable event and policy management system
  - Programmable Full Packet Capture for forensic analysis
  - Visualization of activities, Real-time event notification and actions
- Enforces usage policies
  - Programmable policy management for enforcement

IP Infrastructure Protection

NARUS

- Narus system configured for Real-time network analysis
  - Normalizes across large networks, carrier grade
- Determines anomalous traffic for ensuring continuous network throughput
  - Collects and categorizes network usage from Network to Application layers
  - Programmable threat detection, unauthorized use
  - Baselining of normal network activity, alerts for anomalies
  - Programmable FPC for Forensics analysis
  - Visualization of current historical activity, baselines and anomalies
- Enforcement
  - Supports mitigation techniques



IP Platform for the largest, most Profitable Networks

- Production Proven
  - Tier-1 carrier-grade solutions suite
  - Installed worldwide in multiple configurations
  - Industry-leading mediation and security offerings
- Flexible and Scalable
  - Component and module approach allows flexible and scalable customer specific implementations
  - Standard ability to create and manage highly differentiated mediation and security services
- High Performance
  - Industry leading benchmarked performance, processing 10s of billions of events per day
  - Real-time IP data collection and interactive enforcement

EXHIBIT N

Exhibit N

NARUS™

Unified IP Management & Security

Using the Narus IP Platform to Manage and Secure VoIP Services

Introduction

VoIP is one of many IP based service that Narus can help manage using the Narus IP Platform.

The Narus IP Platform provides a "total network view" of the network traffic, giving IP Carriers visibility into what services are being used on their network, focusing on four functions that are critical to any carrier business – IP Analysis, IP Security, IP Monitoring and IP Mediations

Using the Narus IP Platform carriers can manage and secure the VoIP services in their network. Designed as a multi-tiered and modular architecture, the Narus IP platform can gather and provide highly granular information about each and every VoIP session, in real time, across a large Tier 1 carrier network. This data can be used to create, manage, and protect revenue for the carrier.

Managing and Securing VoIP

The flexibility of the Narus IP Platform allows carriers to create any application they wish; the common uses of the Narus IP Platform to Manage and Secure VoIP services are:

- VoIP Analysis – understanding the VoIP traffic, and details including calling and called party, type of service (SIP, Skype, etc.), gateways used, calling and called party, IP addressed, and more
- VoIP Security – identification of general traffic anomalies, as well as protocol violations
- VoIP Monitoring – targeting and reconstructing (playback) VoIP traffic in either a Lawful Intercept (CALEA) mode, or a Directed Analysis (surveillance) mode. NarusForensics allows the replaying of VoIP traffic for standards based protocols.
- VoIP Mediation – generate revenue from VoIP traffic.

The uses of Narus IP Platform for VoIP are shown in the table below:

Function	Scope	Carrier Use
VoIP Analysis	SIP, H323, Skype, MGCP, others	Ability to collect and process data
VoIP Security	L4 & L7 flood detection, hijacked calls	Security for VoIP service
VoIP Monitoring	VoIP Lawful Intercept, VoIP directed Analysis	Regulatory compliance and ability to intercept VoIP calls
VoIP Mediation	API to billing, provisioning and routing systems	Ability to bill (generate revenue) and manage calls/sessions

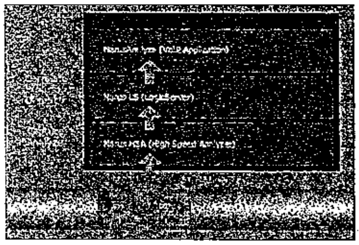
Narus provides benefit in all functions

Narus IP Platform Functionality

The Narus solution is multi-tiered. Within the platform are the first two tiers; the third tier is the application that the platform is enabling. The two Narus tiers or layers are:

- Collection
- Processing

Collection
The collection layer in the Narus solution consists of High Speed Analyzers which connect to the network at the points where the traffic to be monitored can be most efficiently accessed. The Narus HSA's are passive and as such have zero impact on the service delivery. The HSA's analyse each and every IP packet looking at the OSI layer 2 to layer 7 data and extract layer 4 flows and layer 7 application data for every IP session. Appropriate layer 4 and layer 7 data is packaged up and passed to the downstream processing layer as Narus vectors.


NarusAnalyzer (VoIP Application)
Narus LS (LogicServer)
Narus HSA (High Speed Analyzer)

Processing
The processing layer in a Narus deployment is the LogicServer. The LogicServer process runs RuleSets which are programs that apply the business logic to the Narus vectors passed by the collection layer. There are a number of standard RuleSets with the Narus product, plus a SDK that allows customers to modify these, or write custom RuleSets. One or more instance of the VoIP rulesets are used to manage and secure VoIP

VoIP IP Management and Security Applications

Through vector analysis and ruleset processing the Narus IP Platform provides carriers the information they need to know about VoIP services. The table below shows some of the common information carriers need to effectively run their business.

- VoIP Volume over time
- VoIP Percentage
- Volume breakdown – all VoIP volumes broken down by protocol
- Gateways used by VoIP services
- Call length
- Average call length
- Call direction by number
- Call direction by length
- Call direction by volume
- Originating Country by number of calls
- Originating Country by total duration of calls
- International vs. Domestic calls
- Originating IP vs. Gateway by duration
- Terminating IP vs. Gateway by duration
- Latency / QOS
- User name

Use of the Narus IP Platform and VoIP Capabilities

Narus addresses the need, no matter the VoIP services, that the carrier or service provider is offering. The below chart highlights the common uses of the Narus IP Platform VoIP capabilities based on the type of carrier or service provider.

Carrier Provider	Needs	Analyze (Detection)	Mediate (API)	Secure (VoIP Security)	Monitor (VoIP LI/DA)
Wireless Carrier	• Detection • Network security • Fraud • API	✓	✓	✓	✓
Broadband Carrier	• Detection • API • Toll Fraud • Analysis • Network security	✓	✓	✓	✓
VoIP Provider	• LI • Call routing analysis • QoE • QoS (Peering/SLA) • VoIP Security • Fraud • API	✓	✓	✓	✓
IP Carrier	• Detection • Traffic analysis • API • Network (not VoIP) security	✓	✓	✓	✓
WiFi/WiMax Carrier	• Detection • Analysis • API	✓	✓	✓	✓

Uses of the Narus IP Platform

For more information please visit www.narus.com

Or call Narus headquarters in Mountain View CA at 650 230 9300

EXHIBIT O

Exhibit O

NARUS®

UNIFIED IP MANAGEMENT AND SECURITY

SOLUTIONS
NARUS IP PLATFORM
PRESS ROOM
ABOUT NARUS
CONTACT
RESEARCH FELLOWS

Home »

Narus IP Platform

The Narus IP Platform provides:

- **Stateful, Real-Time** analysis of all of the traffic, Layer 3 to Layer 7
- Ability to **target, capture and reconstruct** any session
- **Distributed and scalable, multi-tiered** model
- **Correlates data** from multiples sources, including the network, authentication, and customer records, allowing network managers to analyze traffic and spot trends **across the entire network.**
- **Scalable** across large networks at speeds of **100baseT to 10G / OC192**
- **Development kit** allows customization, to meet any carrier's application requirements

The system is the only carrier class solution that allows customers to instrument their networks once to implement multiple applications. Carriers using the single Narus platform achieve competitive advantages through the quick, effective implementation of applications to:

PROTECT their networks by detecting anomalous events including worms, viruses, DOS, DDOS and other unwanted traffic or malicious attacks

MONITOR and fully reconstruct IP traffic for lawful intercept, surveillance and traffic forensics

ANALYZE traffic in detail for network planning, marketing, and real time management purposes

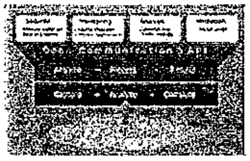
MEDIATE traffic for content and usage-based billing

The Narus IP Platform is the only single solution that enables carrier's focus on the applications that run their business.

*Narus provides the only system that delivers all the functions that carrier class networks require — **Security, Monitoring, Analysis, Mediation,** — **scalable to OC192 / 10G** to meet the requirements of today's networks.*

Diagrams

Click to enlarge:



Download

Narus Backgrounder (PDF)

HOME · SOLUTIONS · NARUS IP PLATFORM · PRESS ROOM · ABOUT NARUS · CONTACT · RESEARCH FELLOWS TOP ^

EXHIBIT P

Exhibit P

NARUS®

UNIFIED IP MANAGEMENT AND SECURITY

SOLUTIONS

IP Security

» NarusSecure

IP Monitoring

» NarusLI

» NarusDA

» NarusForensics

IP Analysis

» NarusAnalyze

» NarusView

IP Mediation

» NarusMediate

NARUS IP PLATFORM

PRESS ROOM

ABOUT NARUS

CONTACT

RESEARCH FELLOWS

Home » Solutions » IP Monitoring

NarusForensics

NarusForensics is used for carrier-class investigative analysis, regulatory compliance and incident response. NarusForensics delivers prompt, solid and actionable security intelligence to Carriers, Law Enforcement and the Intelligence Community.

Key Features

- Reconstructs and renders IP data captured with NarusDA (Directed Analysis), NarusLI (Lawful Intercept) or obtained from other data sources
  - Visually rebuilds or renders web pages and sessions
  - Presents e-mail with the header, body and attachments
  - Plays back streaming video or a VoIP call web session or other interactive medium
- Creates an organized log of all network activities and interprets them into a format that users easily understand
  - Reduces investigation and analysis time from weeks to hours
  - Increases productivity exponentially

Key Benefits

- **Quick and easy incident response:**
  - Corporate, criminal, and intelligence investigations
  - Provides understandable and forensically valid evidence
  - Rapidly discover and produce actionable information
- **Security and regulatory compliance:**
  - Verify effectiveness of policy and technology
- **Intrusion analysis:**
  - Analyze captured traffic for suspicious and "interesting" events

Learn more » NarusLI | NarusDA

NarusForensics delivers prompt, solid and actionable security intelligence to Carriers, Law Enforcement and the Intelligence Community.

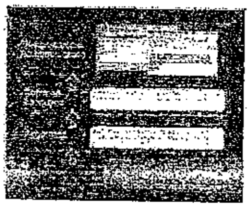
Request Brochure

The following brochure is available by request:

NarusForensics

Diagrams

Click to enlarge:



HOME · SOLUTIONS · NARUS IP PLATFORM · PRESS ROOM · ABOUT NARUS · CONTACT · RESEARCH FELLOWS TOP ^

EXHIBITS Q THROUGH T INTENTIONALLY OMITTED

EXHIBIT U

Exhibit U

NARUS®

UNIFIED IP MANAGEMENT AND SECU

SOLUTIONS
- IP Security
  - » NarusSecure
- IP Monitoring
  - » NarusLI
  - » NarusDA
  - » NarusForensics
- IP Analysis
  - » NarusAnalyze
  - » NarusView
- IP Mediation
  - » NarusMediate

NARUS IP PLATFORM
PRESS ROOM
ABOUT NARUS
CONTACT
RESEARCH FELLOWS

Home » Solutions

IP Security

Public awareness of IP Security for Carrier networks is increasing dramatically with the frequency of attacks and the articles detailing the impact they can have. Carriers know they need to protect their customers with a security solution that is truly scalable, flexible and customizable to address the ever-changing security environment. Only NarusSecure offers a fully scalable solution that addresses their distributed networks at speeds from 100baseT to 10G / OC192.

NarusSecure adds a layer to IP Security i identifying maliciou traffic on Carrier networks at the core

NarusSecure is the only comprehensive carrier class anomaly detection system in the industry addressing DOS, DDOS, Worm, protocol, service, and other sophisticated attacks. Leveraging Narus' powerful IP Platform, NarusSecure reduces detection time while maximizing accuracy rates. This is achieved by correlating data from the data plane (Layer 3 to Layer 7) and the control plane (BGP and IGP) along with other available information.

NarusSecure is the only solution that can be deployed from the core to the edge, providing a truly unique and flexible architecture. By examining all traffic rather than relying on Layer 4 sampling, NarusSecure achieves the highest detection capabilities with the lowest false positive rates in the industry. NarusSecure is the next generation of anomaly detection for Carrier Networks.

Customers

- **AT&T** uses **NarusSecure** to monitor traffic in their backbone, analyzing over 2.6 petabytes of data a day. AT&T is able to provide early warnings to their security center operators, who are able to alert and inoculate their enterprise customers.
- **Korea Telecom** uses **NarusSecure** to help detect harmful traffic and anomalies in their network before the damage is done. With heavy gaming traffic of over 200 million concurrent single packet flows in real time, Narus is the scalable carrier class solution that meets their needs.

Learn more » NarusSecure

HOME · SOLUTIONS · NARUS IP PLATFORM · PRESS ROOM · ABOUT NARUS · CONTACT · RESEARCH FELLOWS

EXHIBITS V THROUGH Z
INTENTIONALLY OMITTED